288-HQ-1242560
MAJ

The following investigation was conducted by Special Agent [redacted] b6 b7C

at Falls Church, VA

Attached are various news articles relating to the above captioned case.

288-HQ-1242560-170

How the FBI tracked down alleged Pentagon hackers

By Rob Lemos, ZDNN
February 27, 1998 6:43 PM PST

The local hunt for the hackers who broke into 11 non-classified Pentagon computers began with a small provider in Santa Rosa, Calif.

"We originally detected the intrusions because the hackers made changes to our operating systems that were easily detectable," said Bill Zane, owner and operator of the 3,000-user Netdex Internet Services in Santa Rosa, Calif. "They were very sloppy in that respect." That was in mid-January.

In the weeks that followed, Zane worked with FBI agents and other network administrators in tracking down the trespassers. "After we figured out they were there, we could have closed up the security holes they were using," said Zane. "Instead, after reviewing the data and seeing the massive scope of it, we decided to take a risk and leave the door open for a while."

MUST SEE ZD

- **FBI's big crackdown nabs small-town teens.**
- **Poulsen: Why hack the Pentagon? Simple. Because it's there.**
- **CyberCrime Interrogation: Ken Geide, new No. 2 anti-hacking cop.**

In fact, "a while" turned into 6 weeks.

The entire time, the FBI kept their dogs on the electronic trail of what they thought could be

TOP STORIES

Updated February 28, 1998 9:58 AM PST

- FBI mounts big crackdown on small-town teens
- Bill to the hill
- No white knight seen for CSC
- HP secures crypto export

E-mail this!
Print this!

potential terrorists. "The FBI had their 10 agents in San Francisco working on overtime over the last month," said Zane. "They considered this to be a very serious issue." Joining the local agent were others from the East Coast where most of the analysis was being done.

Zane, with system administrators from Massachusetts Institute of Technology and UC Berkeley, tracked the intruders and essentially "bugged" their communications. Those messages plus the different mode of operations lead Zane to believe someone is out there -- and they are an adult.

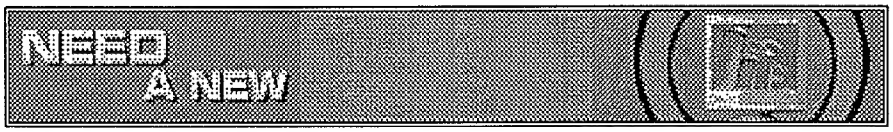
"The other methods were much more sophisticated and acted much more serious," he said.

Top

ZDNN

A ZDNet Site

ZDNET HOME | SITE MAP | SEARCH ZDNET | WHAT'S NEW | AD INFO | CONTACT US



So why hack the Pentagon? Simple. Because it's there

By Kevin Poulsen, ZDNN
February 27, 1998 6:48 PM PST

I was channel surfing last night when I caught the evening news, airing a clip from the 1983 movie *War Games*: Matthew Broderick typing on a keyboard, NORAD going on full alert, worldwide nuclear war looming.

I know what that means. Intruders have broken into yet another low-level Pentagon computer, and examined unimportant and unclassified information, all so they could win bragging rights with their friends.

Time to run for the bomb shelters.

MUST SEE ZD

- **FBI's big crackdown nabs small-town teens.**
- **Road to Cloverdale: How the FBI tracked down Pentagon hackers.**
- **CyberCrime Interrogation: Ken Geide, new No. 2 anti-hacking cop.**

At least one newspaper report suggested that the latest string of Defense Department hack attacks might be the work of the Iraqis. Well, Saddam can breathe a sigh of relief. It turns out the suspects are a couple of teenage hobbyists in Cloverdale, Calif. One of them is 15 years old.

The systems that were cracked housed personnel and payroll data. A Defense Department official characterized the intrusions as a "wake-up call" for increased computer security at the Pentagon. They've been getting this particular wake-up for 15

years now, but someone keeps hitting the snooze button.

And with good reason.

The Defense Department has more computers than God and, as in any large bureaucracy, most of them are not very exciting. Classified systems are isolated from the outside world, physically and electronically and, when it comes to classifying data, the Pentagon errs on the side of caution.

So the only reason anyone would have for cracking a vulnerable Pentagon system is because it's there.

Should youthful adventurers be treated like serious saboteurs? Sadly, that's what is likely to happen ... after a lengthy investigation that will shadow the pranksters as they grow-up, get their first car, and register to vote for the first time.

If the Defense Department wanted to shore up security on its unclassified systems, they could have done it long ago. But then we'd miss the drama of G-men cordoning off a suburban street, and filing out of a *Brady Bunch* home with stacks of floppy disks and modems. We'd miss the chance to give the already-bloated Pentagon budget an extra billion for information security. We wouldn't get to pass new laws cracking down tighter on this grave threat to the American Way of Life.

And we'd never see the **War Games** clip again.

Depending on who you listen to Kevin Poulsen is either a misunderstood former hacker or a menace to society. He writes CHAOS Theory, a weekly column on the electronic underground for CyberCrime.

Top

ZDNN

A ZDNet Site

ZDNET HOME | SITE MAP | SEARCH ZDNET | WHAT'S NEW | AD INFO | CONTACT US

FBI mounts big crackdown on small-town teens

By Robert Lemos, ZDNN
February 28, 1998 11:18 AM PST

The FBI spent six weeks and dedicated more than 20 agents to an effort to track down what it feared to be organized ring of intruders who cracked into Pentagon systems. But after two nighttime raids, the agency found itself dealing with the revelation late Friday that its intensive investigation may have nabbed nothing more than a couple of kids.

During one raid, the agents caught a teen, identified as a 15- or 16-year-old high-school student, in the process of breaking into a non-classified computer system. A second raid targeted the home of another youth suspected of taking part in the Pentagon hacks. The crackdown took place in Cloverdale, a town of some 5,000 residents about 100 miles north of San Francisco.

The two teenagers -- as minors -- were not arrested, but the FBI confiscated computer equipment and software in both homes.

MUST SEE ZD

- **Road to Cloverdale:** **How the FBI tracked down Pentagon hackers.**
- **Poulsen:** **Why hack the Pentagon? Simple. Because it's there.**
- **CyberCrime Interrogation:** **Ken Geide, new No. 2 anti-hacking cop.**

"These are good kids," said Michael Carey, superintendent of the Cloverdale Unified School District. "I'm betting that no charges will be brought against them"

TOP STORIES
Updated February 28, 1998
9:58 AM PST

- FBI mounts big crackdown on small-town teens
- Bill to the hill
- No white knight seen for CSC
- HP secures crypto export

E-mail this!
Print this!

RELATED LINKS
READ
RSA's encryption challenge solved in 39 days
Pentagon hack no surprise
Crypto Crew, Feds at Odds

This ends a chapter in its investigation of several break-ins of unclassified Pentagon computers. The raid occurred the day after Deputy Defense Secretary John Hamre revealed that 11 unclassified Pentagon systems had been broken into earlier this month.

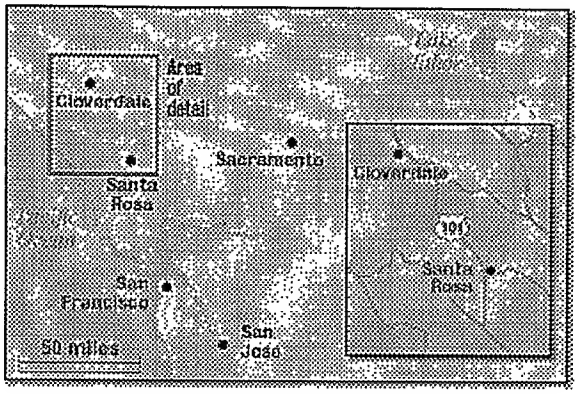
According to federal investigators, other Cloverdale High students are in the process of being questioned by Secret Service and FBI agents. The suspicion is that the hacking was being conducted by a ring of youths, who may have been in a contest to see who could get farthest into government computers.

"Most everyone here is thinking that this was some kind of computer contest" said one student at Cloverdale High School.

Earlier this week, Deputy Defense Secretary Hamre stated that the online trespasses were "the most organized and systematic attack the Pentagon has seen to date."

"This says amazing things about the kids' skills and really poor things about the Pentagon's security," said a hacker unrelated to the incidents, who preferred to be identified by his online name, darkcube.

But the hunt isn't over -- at least not according Bill Zane, who owns the 3,000-user Netdex Internet Services in Santa Rosa, Calif. The hackers apparently broke into Netdex on the way to the Pentagon. In fact, Zane may have given FBI agents their first bead on the intruders. "There's at least one more and most likely two more out there," Zane said. "It's not just these two kids."



Zane, with system administrators from Massachusetts Institute of Technology and UC Berkeley, tracked the intruders and essentially "bugged" their communications. Those messages plus the different mode of operations lead Zane to believe someone is out there -- and they are an adult.

"The other methods were much more sophisticated and acted much more serious," he said.

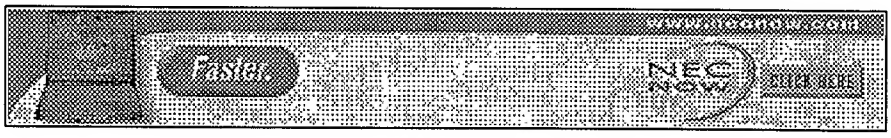
As for the two young hackers, worse crimes could have been committed. "I would have much more concerned if they had hacked the school system or tampered with grades," said Superintendent Carey. "It was more an innocent game than a malicious attack."

Alex Wellen, ZDTV CyberCrime, contributed to this report.

Top

A ZDNet Site

ZDNET HOME | SITE MAP | SEARCH ZDNET | WHAT'S NEW | AD INFO | CONTACT US



288-HQ-1242560
MAJ

The following investigation conducted by Special Agent [redacted]

at Falls Church, VA

An Internet news story attributed to "The Australian Online" dated October 21 1997, by [redacted] was obtained which indicates that [redacted] pleaded guilty to charges which carry a 10 year sentence. [redacted] plead guilty in Sydney District Court to the main offence under Section 76E of the Crimes Act for his hacking into an Australian ISP named AUSnet, changing their web page, and distributing their clients' credit card details across the Internet. Damages resulting from this incident are estimated to be $2 million. An additional eight charges are also indicated. [redacted] is reported to be sentenced in November 1997 for offenses related to other charges he faces on making $50,000 worth of illegal phone calls by tapping into the public telephone system. [redacted] hacker name is [redacted] and he is [redacted] years old. [redacted] is scheduled to be sentenced on February 5, 1998. A copy of this Internet news story is attached.

b6
b7C

A second Internet news story was obtained which also describes the legal status of [redacted] This story was contained in an email message dated 2/10/98 which was sent through an anonymous remailer. The story indicates the author to be [redacted] This story contains the following information: [redacted] of Sydney, Australia, is to be sentenced "today" for charges of hacking into the ISP AUSnet and circulating the information on 1200 credit cards onto the Internet. [redacted] faces a maximum 10 year sentence in the Downing Centre District Court. Damages estimated to be $2 million in lost clients and contracts. [redacted] hacked into AUSnet in March 1995, two months after he was refused a job with AUSnet. [redacted] faces 1 count of inserting data into a computer, which carries a maximum 10-year sentence, and 8 counts of unlawful access to computer data. A copy of this news story is attached.

288-HQ-1242560-173

Optik Surfer faces 10 years for hack attack

By GEOFF LONG

October 21: Optik Surfer – the hacker who broke into the system of ISP AUSnet and distributed clients' credit card details across the Internet – has pleaded guilty to charges carrying a maximum penalty of 10 years imprisonment.

The Australian Federal Police computer crime unit spent more than six months in 1995 tracking down the hacker, who also altered the AUSnet Web site and sent e-mail messages from the system administrators' account. Computer crime agents spent almost 12 months preparing the case against the hacker.

Skeeve Stevens, a 27-year-old computer consultant, was charged with eight counts of gaining unlawful access to computer data and one count of inserting data into a computer system.

Stevens pleaded guilty in Sydney District Court to the main offence under Section 76E of the Crimes Act, which carries a 10-year sentence, and asked the court take the other eight charges into consideration when sentencing.

It is the second time in the past month that a hacker has pleaded guilty in court.

Next month another hacker will be sentenced for offences related to making up to $50,000 worth of illegal phone calls by tapping into the public telephone system.

Graham Henley, a former agent with the Australian Federal Police computer crime unit who now heads computer forensic services for Network Security Management, was involved in both cases.

Mr Henley tracked the source of the Optik Surfer attack to a computer laboratory at Monash University.

The court was told that after the break-in, the hacker returned to the system and sent an e-mail message to journalists from an account operated by AUSnet's technical director.

Identifying himself as the Optik Surfer, he boasted of his break-in and said that the credit card details had been distributed to highlight the poor security at AUSnet.

AUSnet's Web site was also altered to greet visitors with the quote: "Remember – too

many secrets."

The quote comes from Sneakers, a 1993 film about hackers starring Robert Redford.

Stevens originally denied being the hacker but claimed to the media that he was in contact with the so-called Optik Surfer.

Mr Henley was aware of Stevens as a result of a previous conviction for computer hacking.

Federal police alleged that Stevens' actions cost AUSnet more than $2 million in contract losses.

Banks had had to re-issue many of the credit cards.

The matter was adjourned for sentencing on February 5 next year.

TOP HOME

288-HQ-1242560
WME:wme wme

1

On March 5, 1998 [redacted] contacted Special Agent [redacted] by telephone. CS then furnished the following information:

CS discovered an online news article which includes an interview with the hacker named Analyzer. The address for this web page is http://www.antionline.com/PentagonHacker/HackerStory2.html. This is an interview conducted on an Internet chat service between Analyzer and another person using the name JP.

b6
b7C
b7D

SA [redacted] subsequently visited this Internet site and printed the interview. That material is attached to this insert.

288-HQ-1242560-176

288-HQ-1242560
MAJ

The following investigation was conducted by Special Agents (SA) [redacted] and [redacted],

at Falls Church, VA

On 02/19/98 [redacted] of Georgetown University, Computer Science Department, was interviewed at her place of employment, Georgetown University, Washington, DC 20057. SA [redacted] advised [redacted] that the [redacted] account at Georgetown University could have been compromised on 12/19/97 and 02/12/98. [redacted] advised that she would advise the system administrators of the Georgetown accounts of this information.

b6
b7C

On 02/20/98 [redacted] advised SA [redacted] that the system administrator, [redacted] checked the [redacted] account. [redacted] advised that the [redacted] account did have any unusual logins on the dates that SA [redacted] provided. The 12/19/97 was a login from Georgetown University and the 02/12/98 login was a dial-up SLIP (Serial Line Internet Protocol) connection.

288-HQ-1242560-177

288-HQ-1242560
MAJ

The following investigation conducted by Special Agent [redacted] b6 b7C

at Falls Church, VA [redacted] b3 OTHER Sealed pursuant to court order

On 02/17/98, per [redacted] provided [redacted] (attached).

On 02/18/98, inquires to the NATIONAL CRIME INFORMATION CENTER (NCIC) INTERSTATE IDENTIFICATION INDEX (III) were negative regarding any criminal identifiable with [redacted] Date of Birth [redacted]

On 02/18/98 inquires to the VIRGINIA DEPARTMENT OF MOTOR VEHICLES disclosed the following information regarding [redacted] Date of Birth [redacted]:

[redacted] b6 b7C

On 02/18/98 inquires to the MARYLAND DEPARTMENT OF MOTOR VEHICLES disclosed no record regarding [redacted] Date of Birth [redacted]

On 02/18/98, inquiries to the LEXIS-NEXIS PERSON LOCATOR database disclosed the following regarding [redacted] permanent address, [redacted]

RESIDENT(S)	APPROXIMATE BIRTH DATE
[redacted]	

288-HQ-1242560-179

[redacted]

On 02/18/98, inquiries to the LEXIS-NEXIS PERSON LOCATOR database disclosed the following names listed with [redacted] local address, [redacted] which is a [redacted] dwelling:

[redacted]

b6
b7C

On 02/18/98 inquires to the AUTOMATED CASE SUPPORT (ACS) system disclosed negative results regarding [redacted]

On 03/02/98 [redacted] FBIHQ, made an inquiry to the IMMIGRATION AND NATURALIZATION (INS) database located at FBIHQ, National Security Division, and advised that there is no record of [redacted] in the INS database.